UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,345	02/24/2004	William J. Yeager	SUN040417	3832

24209 7590 12/31/2008

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER	
TABOR, AMARE F	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
12/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,345	YEAGER ET AL.	
	Examiner	Art Unit	
	AMARE TABOR	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This correspondence is in response to **Amendments** and **REMARKS** filed on Oct'17, 2008.

2. Claims 35, 36, 41 and 42 are amended; and **Claims 1-42** are pending.

Response to Arguments

3. Applicant's arguments filed on 10/17/2008 have been fully considered but they are not persuasive.

Applicants' argued that "*An intermediary peer node, also called a '**super peer**' or '**super peer node**', is defined in Applicants' Specification… Applicants respectfully submit that the Examiner has failed to show where in **Vigue** reference, the **Winget** reference, or any proper combination of the **Vigue** reference and the **Winget** reference, an intermediary peer node, as defined in Applicants' specification, is described, disclosed, taught or suggested.*" Examiner respectfully disagrees.

First, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., '***super peer***' *or* '***super peer node***') are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Second, the invention claims [see claim 1, for example]: *A method of securing communication between peers in a P2P network, where: (i)the peer node generating a secured communication request to the intermediary peer node; then (ii) the intermediary peer node authenticating the peer node in response to said secured communication request; and then (iii) the intermediary peer node issuing a signed certificate of authority upon successful authentication.*

As best understood from the claim language and with broadest-reasonable claim interpretation - the invention simply claims peer nodes mutually authenticating each other. Specifically, the secondary

peer node [which could be an intermediary peer node, or another peer node or a server on the P2P network] authenticating the first peer node. Thus, as indicated in the last office action, **Vigue** discloses a P2P network [see FIGS.1 and 3-4B] where a requesting peer node generates a communication request to a responding peer node. Additionally, **Vigue** discloses the responding peer verifying the communication request of the requesting peer node [see FIG.8 and abstract]. On the other hand, **Winget** discloses a P2P network where a server and a peer mutually authenticating each other. Therefore, a person of ordinary skill in the art can assert that the applied references clearly disclose the claimed features of the invention.

4. Applicant's arguments with respect to the objection of claims 11, 22 and 33 have been fully considered and are persuasive. Therefore, the objection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of 35 U.S.C., 112 2nd paragraph.

Claim Objections

5. **Claim 42** is objected to because of the following informalities: Please correct or clarify the limitation "*receive a secured communication request from an peer node*". For examining purposes, the limitation is read as, "*receive a secured communication request from an intermediary peer node*". Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 11, 22 and 33 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 11, 22 and 33 contain the trademark/trade name **JXTA**. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not

comply with the requirements of 35 U.S.C. 112, second paragraph. See *Ex parte Simpson*, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, that the trademark/trade name, JXTA, is used to identify/describe a project and architecture name/trademark [as Applicants indicated in the last response filed on 10/17/2008] and, accordingly, the identification/description is indefinite.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-10, 12-15, 17-21, 23-26, 28-32 and 34-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vigue et al. (US 2003/0163702 A1 - "Vigue") in view of Winget et al. (US 2005/0120213 A1 - "Winget")

As per Claim 1, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: the peer node generating a secured communication request to the intermediary peer node [see abstract]; and the intermediary peer node issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses intermediary peer generating response to said communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, in the same field of endeavor, **Winget** discloses intermediary peer node authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of peer node authentication in order to establish a secure communication tunnel between peers [see at least abstract of **Winget**].

As per Claim 12, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to a secured communication request to the intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11]. On the other hand, **Winget** discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 23, Vigue teaches,

A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method comprising: receiving a secured communication request from the peer node [see abstract, lines 3-7]; and sending a

singed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, **Winget** discloses authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 34, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030], the method including: the peer node generating a secured communication request to the intermediary peer node [see abstract, lines 3-7]; and the intermediary peer node issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses intermediary peer node generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, **Winget** discloses peer node authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 35, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to- peer networks [see FIGS.1 and 2; and for example, par.0029 and 0030], the method including receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating a secured communication request to an intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11]. On the other hand, **Winget** discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 36, Vigue teaches,

A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to- peer networks [see FIGS.1 and 2; and for example, par.0029 and 0030], the method including: an intermediary peer node receiving a secured communication request from the peer node [see abstract, lines 3-7]; and sending a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, **Winget** discloses authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 37, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for generating a secured communication request to the intermediary peer node [see abstract, lines 3-7], and means for issuing a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, **Winget** discloses authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 38, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for receiving a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating a secured communication request to the intermediary peer node [see FIGS.3-4B; and for example, abstract, lines 3-11]. On the other hand, **Winget** discloses authenticating the peer node in response to said secured communication request [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of

authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 39, Vigue teaches,

An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network [see FIGS.1 and 2; and for example, par.0029 and 0030] comprising: means for receiving a secured communication request from the peer node [see abstract, lines 3-7]; and means for sending a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses means for generating response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other hand, **Winget** discloses authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 40, Vigue teaches,

A peer-to-peer network system comprising: a peer node [see FIGS.1 and 2]; an intermediary peer node communicatively coupled to said peer node [see FIGS.1 and 2]; wherein said peer node is configured to generate a secured communication request to said intermediary peer node [see abstract, lines 3-7]; and wherein said intermediary peer node is configured to issue a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses wherein said intermediary peer node is configured to generate response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 8-11]. On the other

hand, **Winget** discloses authenticate said peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 41, Vigue teaches,

A peer node comprising: a processor [see FIGS.1 and 2 – *which includes inherent processor*. See also **PROCESSOR 1051** in FIG.10]; and a memory [see **MEMORY 1053** in FIG.10] comprising program instructions, wherein the program instructions are executable by the processor to: generate a secured communication request to the intermediary peer node capable of authenticating the peer node in response to said secured communication request [see abstract, lines 3-11], and receive a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses generate a secured communication request to an intermediary peer node in response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 3-11]. On the other hand, **Winget** discloses authenticating the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claim 42, Vigue teaches,

An intermediary peer node comprising: a processor [see FIGS.1 and 2 – *which includes inherent processor*. See also **PROCESSOR 1051** in FIG.10]; and a memory [see **MEMORY 1053** in FIG.10] comprising program instructions, wherein the program instructions are executable by the processor to: send a signed certificate of authority upon successful authentication [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract, lines 11-16].

Vigue discloses receive a secured communication request from an intermediary peer node; and generate response to said secured communication request [see FIGS.3-4B; and for example, abstract, lines 3-11]. On the other hand, **Winget** discloses authenticate the peer node [see FIG.1; and for example, abstract]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of Applicants' invention, to modify the system of **Vigue** by incorporating **Winget's** teaching of authentication so that a secure communication tunnel is established between peers [see abstract of **Winget**].

As per Claims 2 and 3, Vigue-Winget combination teaches,

wherein said secured communication request comprises a certificate signing request, wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request [see **VERIFY INTEGRITY OF RETRIEVED DATA 248** in FIG.8; and for example, abstract of **Vigue**], a unique identifier [see **version identifier** in abstract of **Vigue**], and a password [see par.0003, 0007 and 0121 of **Winget**].

Claims 13-14 and 24-25 are rejected for the same reasons applied to the rejection of Claim 3.

As per Claim 4, Vigue-Winget combination teaches,

wherein said secured communication protocol comprises a transport layer data authentication protocol [see **TLS** in FIGS.3 and 4 of **Winget**].

Claims 15 and 26 are rejected for the same reasons applied to the rejection of Claim 4.

As per Claims 6 and 7, Vigue-Winget combination teaches,

securing a pipe connection between the peer node and the intermediary peer node upon authentication [see FIGS.1 and 6 of **Winget**]; and closing said pipe connection upon failed authentication of said node [see **CANCELLING REQUEST 128** in FIG.3 of **Vigue**].

Claims 17-18 and 28-29 are rejected for the same reasons applied to the rejection of Claim 7.

As per Claims 8-10, Vigue-Winget combination teaches,

wherein said peer node comprises a peer node advertisement and a pipe node advertisement; wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information [see **TLS** in FIGS.3 and 4 of **Winget**]; and wherein said pipe node advertisement includes an application-dependent port identifier [see **Carrier Protocol** in FIG.3 of **Winget**], said unique identifier, a name, and a type [see FIGS.4 and 5 of **Winget**].

Claims 19-21 and 30-32 are rejected for the same reasons applied to the rejection of Claim 8.

Claims 5, 11, 16, 22, 27 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Vigue" in view of "Winget", and further in view of Rutherglen et al. (US 2003/0033517 A1 - "Rutherglen")

As per Claim 5, Vigue-Winget combination teaches,

authenticating the peer node in response to said secured communication request [see abstracts of Vigue and Wignet], but fails to disclose wherein said intermediate peer node is communicatively coupled to an enterprise database. Nevertheless, in the same field of endeavor, **Rutherglen** discloses wherein said intermediate peer node is communicatively coupled to an enterprise database [see **DATABASE SERVER** in FIGS.1, 2 and 3B-6]. It would have been obvious to modify the system of **Vigue-Winget** by incorporating the DATABASE SERVER of **Rutherglen** in order to have a direct access to the database that is protected by a security system [see at least abstract; and for example, par.0001 of **Rutherglen**].

Claims 16 and 27 are rejected for the same reasons applied to the rejection of Claim 5.

As per Claim 11, Vigue-Winget combination teaches,

operating peer-to-peer network [see abstracts of **Vigue** and **Wignet**], but fails to disclose using a JXTA technology-enabled platform. Nevertheless, **Rutherglen** discloses using a JXTA technology-enabled platform [see par.0013 and 0108]. It would have been obvious to modify the system of **Vigue-**

Winget by incorporating JXTA teachings of **Rutherglen** in order to implement a network protocol that would inter-operate with any peer [see par.0109 of **Rutherglen**].

Claims 22 and 33 are rejected for the same reasons applied to the rejection of Claim 11.

CONTACT INFORMATION

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to AMARE TABOR whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Amare Tabor
(AU 2439)

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434